2

(Unclassified Paper)

NAVAL WAR COLLEGE
Newport, R.I.

A MODEL FOR THE EMPLOYMENT OF MICROCOMPUTER SYSTEMS IN OPERATIONAL DECEPTION SCENARIOS

by

James E. Vesely

LtCol, USMC

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: James E Vesely

18 May, 1992

Paper directed by COL R.E. Heim, USA,
Professor, Operations Department

Approved by:

______________________ ____________
COL R.E. Heim Date

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION
UNCLASSIFIED

1b. RESTRICTIVE MARKINGS

2a. SECURITY CLASSIFICATION AUTHORITY

2b. DECLASSIFICATION / DOWNGRADING SCHEDULE

3. DISTRIBUTION / AVAILABILITY OF REPORT
DISTRIBUTION STATEMENT A: Approved for Public Release; distribution is unlimited.

4. PERFORMING ORGANIZATION REPORT NUMBER(S)

5. MONITORING ORGANIZATION REPORT NUMBER(S)

6a. NAME OF PERFORMING ORGANIZATION
OPERATIONS DEPARTMENT

6b. OFFICE SYMBOL (If applicable)
C

7a. NAME OF MONITORING ORGANIZATION

6c. ADDRESS (City, State, and ZIP Code)
NAVAL WAR COLLEGE
NEWPORT, R.I. 02841

7b. ADDRESS (City, State, and ZIP Code)

8a. NAME OF FUNDING / SPONSORING ORGANIZATION

8b. OFFICE SYMBOL (If applicable)

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

8c. ADDRESS (City, State, and ZIP Code)

10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification) A MODEL FOR THE EMPLOYMENT OF MICROCOMPUTER SYSTEMS IN OPERATIONAL DECEPTION SCENARIOS (U)

12. PERSONAL AUTHOR(S) LTCOL JAMES E. VESELY USMC

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
FINAL	FROM ________ TO ________	1992 MAY 18	37

16. SUPPLEMENTARY NOTATION A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Operations. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

17. COSATI CODES

FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
CD-ROM COMMUNICATIONS DECEPTION EMISSIONS ELECTRONIC COUNTERMEASURES MODEL OPERATIONS SCENARIO RADIO

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

This paper suggests a model for the employment of microcomputer systems in support of operational deception. In establishing the case for such a model, a discussion is presented which lays the foundation for sound, realistic operational deception through the use of radio communications. An opinion is presented that both past and current practices in this field have been inefficient and lack realism when directed against even a mildly proficient opponent. A view and discussion is provided of the current manual-intensive model for operational deception which explains its shortcomings and deficiencies. Based on the current state of microcomputers technology in the Armed Forces of the United States, a model is proposed which is centered around the technology. The proposed model takes advantage of the computer's ability for scenario management, mass storage capability, and device control. A proposal is made which could lead to a systems development effort which would engineer the software components and identify the hardware requirements for the implementation of the proposed model. The conclusion pionts to the advantages and options such an implementation would provide to the operational commander.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS

21. ABSTRACT SECURITY CLASSIFICATION
UNCLASSIFIED

22a. NAME OF RESPONSIBLE INDIVIDUAL	22b. TELEPHONE (Include Area Code)	22c. OFFICE SYMBOL
CHAIRMAN, OPERATIONS DEPARTMENT	841-3414	C

83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

Abstract of

A MODEL FOR THE EMPLOYMENT OF MICROCOMPUTER SYSTEMS IN OPERATIONAL DECEPTION SCENARIOS

This paper suggests a model for the employment of microcomputer systems in support of operational deception. In establishing the case for such a model, a discussion is presented which lays the foundation for sound, realistic operational deception through the use of radio communications. An opinion is presented that both past and current practices in this field have been inefficient and lack realism when directed against even a mildly proficient opponent. A view and discussion is provided of the current manual-intensive model for operational deception which explain its shortcomings and deficiencies. Based on the current state of microcomputer technology in the Armed Forces of the United States, a model is proposed which is centered around this technology. The proposed model takes advantage of the computer's ability for scenario management, mass storage capability and device control. A proposal is made which could lead to a systems development effort which would engineer the software components and identify the hardware requirements for the implementation of the proposed model. The conclusion points to the advantages and options such an implementation would provide to the operational commander.

PREFACE

My research has determined that there is virtually no literature in the public domain that addresses the subject of automated electronic communications deception. As a result, no formal models for this subject area are to be found. A few organizations in each of the services, mostly communications battalions and electronic warfare units heavily involved with Electronic Countermeasures (ECM) and Electronic Counter-Counter Measures (ECCM), have localized standard operating procedures dealing with manual scenarios for radio and radar deception. These are almost entirely based on ad hoc and informal efforts by individuals working on their own initiative based on practical experience. Therefore, the majority of the material listed in the Bibliography only provides a basis for the deception principles upon which I based my research.

TABLE OF CONTENTS

CHAPTER PAGE

LIST OF ILLUSTRATIONS

A MODEL FOR THE EMPLOYMENT OF MICROCOMPUTER SYSTEMS IN OPERATIONAL DECEPTION SCENARIOS

CHAPTER I

INTRODUCTION

Sun Tzu: "All warfare is based on deception."[1]

Clausewitz: [Deception] "...should not be considered as a significant independent field of action..."[2]

Here are two of the most preeminent military strategists telling us very different things about deception in warfare. Those who would want to make a case for the use of deception in the conduct of operations could dust off their copy of The Art of War and quote the elegant passages contained therein. On the other hand, those who place no value in deceptive maneuvers and consider them a waste of time can turn to Carl von Clausewitz's On War for strong support. Well, not so fast. As Professor Handel explains so well in his work comparing these two strategists, Clausewitz was convinced that deception at the strategic level of war was virtually impossible. At the operational level, Clausewitz considered deception, and the resultant surprise achieved, fundamental.[3] It is at the operational level of war that this paper presents a model for the use of microcomputers as a deception tool.

During the World War II, in preparation for the invasion of Normandy, General Eisenhower's staff directed a radio electronics deception which helped convince the Germans that the invasion was most likely to take place at the Pas de Calais. A deception cell was located in Southeast England at a place where it was natural to assemble units for the quick transfer of troops and supplies to France near Calais. Through the use of written scripts and ad hoc transmissions, the allies were able to simulate the existence of a bogus US Army Group called "FUSAG". This deception plan was successful in helping to convince the Germans to hold their Fifteenth Army in the vicinity of Calais far past the time of the actual landings at Normandy.[4]

This example illustrates how Americans endeavor to plan and conduct campaigns. Units are usually spread throughout the area of operations, either in their assembly areas, the communications zone or maneuvering to contact. In this environment, radio communications plays a key role in command and control. Simply put, the American way of war involves a plethora of combat and combat service support units that emit considerable amounts of radio-based electromagnetic radiation.

On the other hand, we also take great pains to prevent an opposing force from gathering intelligence concerning U.S. force location, disposition and intentions. In short, we try to blind the enemy both in the air and on the ground. If the efforts to do so are successful, the enemy is kept at arm's length such that he cannot physically gain information about U.S. forces. But, even with these efforts, there is one way that even a mildly capable enemy force can acquire substantial information regarding our forces and that is through the reception and analysis of the electromagnetic radiation emanating from our headquarters, logistics bases and troop concentrations.

Even some of our relatively unsophisticated enemies will possess effective direction finding and electronic information gathering capabilities. Most low to mid level conflicts will involve an enemy who can translate the electronic information into usable military intelligence. Considering these situations, it is evident that opportunity is presented to the American military campaign planner for the employment of a comprehensive radio communications deception operation. If the enemy can be physically precluded from gathering information on our military posture in that he is unable to see what we are doing, we can use communications ruses very effectively. Due to the natural laws surrounding electronic radiation, it is near impossible to prevent an enemy from at least intercepting the emissions.

These two situations, a blinded enemy and his capability to intercept electronic emissions, play into the hands of the American commander who wishes to employ electronic deception because the enemy commander is forced into a situation where he must rely almost entirely on the intelligence gathered by electronic means. The smart commander will take advantage of these circumstances when planning a campaign.

Automated systems which would aid the operational commander in the execution of a communications based deception plan are almost entirely non existent. One would think that the highly technical nature of such an endeavor would surely lend itself to the application of automated systems technology. In my research on this topic, I could find only one computer based automated system directed at this effort and that system, currently in the development stage, was a tool for deception planning only. It did nothing to aid the communicators or the deception cell personnel in the execution of a plan.

Believing strongly that deception at the operational level of war is a true force multiplier and that computer automation can greatly aid in the execution of deception scenarios, this paper will propose a model for the application of current automated technology to the subset of deception dealing with electronic radio communications. To establish a baseline for the model, this paper will describe the problems with past practices in radio communications deception. In response to these problems, the paper will detail the desired components of the model with an explanation of each component. Both advantages and disadvantages of the model are presented. Finally, the paper will provide some conclusions regarding the research.

CHAPTER II

THE PROBLEM WITH CURRENT PRACTICES

There would be no need to propose a structured model for radio communications deception if the current method of implementation were any where near optimal. However, this is not the case. Like most deception schemes, communications deception is not given much credence except when it becomes imperative or, at least, highly desirable as a component of an operation. This is understandable since it is costly, both in human and equipment resources, to train in this discipline. Also, the results of canned training exercise deceptions, as elaborate as they tend to be at the operational level of warfare, are not easily discernible or determinable. Even in larger scale force on force exercises, the benefits of a successful radio emissions deception are hard to evaluate. Because of these difficulties, little attention is paid to the force multiplication advantages accrued through realistic communications deception.

This issue is at the heart of Clausewitz's problems with deception at the operational level of war. He writes:

> "To prepare a sham action with sufficient thoroughness to impress an enemy requires a considerable expenditure of time and effort, and the costs increase with the scale of the deception.[5]

The key phrase here is "sufficient thoroughness". Without it there can be no realism to the deception. The contention here is that today's commander does not have the proper resources or tools to conduct a thorough radio communication deception at the campaign level

Besides a lack of attention, this form of deception, as presently practiced, is less than optimal because of the mechanics involved. Scenarios are usually plucked from the last command post exercise conducted by the unit to be imitated. The "yellow canary" message traffic notes are assembled into as best a sequence as possible, given the time available, then parceled out to whatever operator is to transmit them. Content and sequencing are not always considered so issues such as tempo, synchronization and diversity are not addressed or, addressed so lightly that they result in a lack of realism.

Since human resources are always at a premium, there may not be enough scenario directors, radio operators, radio talkers and drivers to conduct the deception. Volume and control suffer as a result. Worse yet, there will never be enough staff and communications specialists which can be dedicated to the construction of the radio deception scenario. Without the dedication and expertise of such people in the design of the deception key elements such as footprints, signatures, patterns, content and, above all, realism will be degraded. For an understanding of these key elements, see Appendix I.

There is never any time allotted for review and evaluation in the development of a radio communication deception. No one can say for sure, beforehand, just how realistic the radio emissions will be for a given deception. Designs are quickly put together, usually on the spot, without time for inspection and adjustment. Deception teams are normally ad hoc groupings of extraneous personnel who are usually unfamiliar with the unit that they are to imitate. Equipment is scratched up from whatever stocks can be safely released by operational units. The deceivers are left to do the best they can.

If the deception scenario was designed and developed by a team of specialists and written down in scripts and made available to the operational commander and his staff prior to the campaign, it would be a significant advantage over the ad hoc implementation which is normally the case. However, a rapidly changing situation in the commander's area of responsibility might negate the one or two scenarios which could be "canned" for the operation. Flexibility is what is needed in the availability of catalogued radio communications deception. With the proper tools, a commander and his staff could have an almost inexhaustible selection of unit types, activities and battlefield situations to choose from.

In the future, the operational commander will have fewer and fewer resources at his disposal. This is especially true as regards human resources. Therefore, a solution for the implementation of radio communications deception based in current and future microcomputer technology appears to be desirable. The objective of any such solution must be to maximize the commander's options in this area of deception while easing his requirement for personnel dedicated to the effort. Furthermore, the solution must provide a robust, flexible and realistic set of outputs. A model for such a solution is presented in the next chapter.

CHAPTER III

THE PROPOSED MODEL

As is the case with most every automated system, the proposed model is comprised of a combination of functions, hardware and software components, and procedures. Following an executive overview, the major functions of the model will be presented. Then, in order to understand the uses for the model, various operational configurations and modes will be presented along with a description of the components which constitute the model itself.

OVERVIEW

What technological changes have come about such that a microcomputer based model for radio communications deception is being proposed? More than one would imagine, considering that microcomputers have been around for more than twenty years. It is the combination of faster speed, variety in output device interfaces, tremendously increased storage capacity and, most of all, advances in the digitalization of sound and images that allow for a proposal such as the one contained in this paper. Since its inception, the microcomputer has had the capability for electronic management of such an environment but, it did not have the capacity required for the storage and manipulation of the volumes of data required to emulate a large scale radio deception which would be useful at the operational level of warfare.

Today's electronic equipment milieu, offering up such powerful devices as high capacity microcomputers, multi-functional modems, digital radio networks, packet switching radios, software controlled encryption devices, compact disk (CD) players and potent software packages places a system such as described in the proposed model in the realm of reality.

Today's microcomputer speed and storage capacity provides for large, highly functional programs which can manage deception scenarios. The advent of the CD player, with its capacity for storage of untold quantities of digitized sound, makes available a usable database of radio traffic messages. Communications equipment (radios, modems, encryption devices) that operate in digital, vice exclusively analog environments, allow for the pliable manipulation of propagated radio traffic. Digitized data is highly malleable in comparison to analog data; especially through the use of microcomputers. In combination, these subsystems (microcomputer, CD players and digital radio networks) provide the foundation for the proposed model.

FUNCTIONS PERFORMED BY THE MODEL

In order to take maximum advantage of the technology available to us, we look to three major areas of functionality for the model. The first centers on the data which is the basis of the deception, i.e., the radio message traffic. Next, the data must be tied together in some coherent manner to produce a deception scenario which is usable. And, finally, we would want the model to be able to execute and control the deception for us in the most automated manner possible.

A radio communication deception scenario is based on the quantity, content and propagation of radio message traffic. To facilitate this basis the model must be able to capture, catalogue and store messages which can then be retrieved and transmitted. In order for the message traffic data to be manipulated by the automated system, it has to contain enough intelligence so that the system knows the nature of the data it is dealing with. Figure 1 presents a model for the stored message traffic data in this system.

Each element in the message traffic frame contains information which is of use to the deception scenario builder

MESSAGE #	MESSAGE TYPE	MESSAGE LINK	MESSAGE TRAF TEXT ....

MESSAGE TRAFFIC FRAME EXAMPLE

FIGURE 1

and execution modules of the system. The message is identified by a unique number for cataloging by the MESSAGE # field. MESSAGE TYPE identifies the message content, possibly as a tactical message for a corps level G-3 application or a logistics or administrative message. MESSAGE LINK provides linkage to a follow-on message or a required response to the traffic contained in the text. Finally, the TEXT field stores the message body itself.

An automated application to capture and catalogue message traffic would have to be developed and this is considered the most challenging of the tasks associated with the proposed model. Radio traffic would have to be recorded, digitized and have the control data appended to it for eventual storage on a CD. All of the elements of realistic deception described in Appendix I would have to be taken into consideration. Formidable as the task seems, once automated procedures are in place to aid in the construction of the message traffic database, it could certainly be accomplished. Message traffic from unit exercises, recorded on audio tape, could be transferred to the CD medium to provide the substance for the database. There is this significant up front cost associated with the construction of databases but, once built the individual message frames can be used over and over again in various applications. The output product of this function of the model is one or more radio message databases, each reflecting the operational functionality of a unit in the conduct of a mission.

With the message traffic database as the raw materiel for the deception, the model must provide a function to tie the messages together into a coherent scenario. This function is performed by a "scenario manager", an application software package that builds the scenario script and stores it on a script database for eventual execution. The deception administrator, a specialist who is versed in the development of radio communications deceptions, uses the scenario manager software to construct and store the scenario. To tie the messages together into a scenario, control data is appended to the message number which directs the message traffic during the scenario.

Figure 2 depicts a notional scenario control frame. Control data associates the stored message traffic with a specific scenario, determines its required destination and provides additional information which could contain instructions for a receiving node. Special instructions might include movement direction such as "move your node to location DELTA" or "transmit message KQL87134" and the like. Also, these instructions might contain broadcast media information

SCENARIO NUMBER	MESSAGE #	DESTINATION NODE	SPECIAL INSTR

SCENARIO CONTROL FRAME EXAMPLE

FIGURE 2

such as "send this message encrypted over VHF radio". The output of the scenario manager is a scenario database which is the digitally stored version of the planned radio communications deception.

Lastly, a function is required which will execute the stored deception scenarios. In the model, this is designated as the "deception manager". Each automated node in the deception network will contain a management software package with the central node manager controlling the subnodes by the propagation of control frame data along with the radio message traffic. Simply put, the deception managers conduct the deception by manipulation of the data stored on the scenario database. It is the interaction of the various deception managers in the network, based on the intelligence and message traffic stored in the system, which makes up the radio communication deception. When the deception management software retrieves a message frame, it acts according to the data stored in it. Based on this data, the manager might direct a frame of voice data to an unencrypted VHF radio for transmission. A receiving node, captures this transmission, and its associated control data, and acts accordingly; the subnode might transmit a response to the message after a specified amount of time.

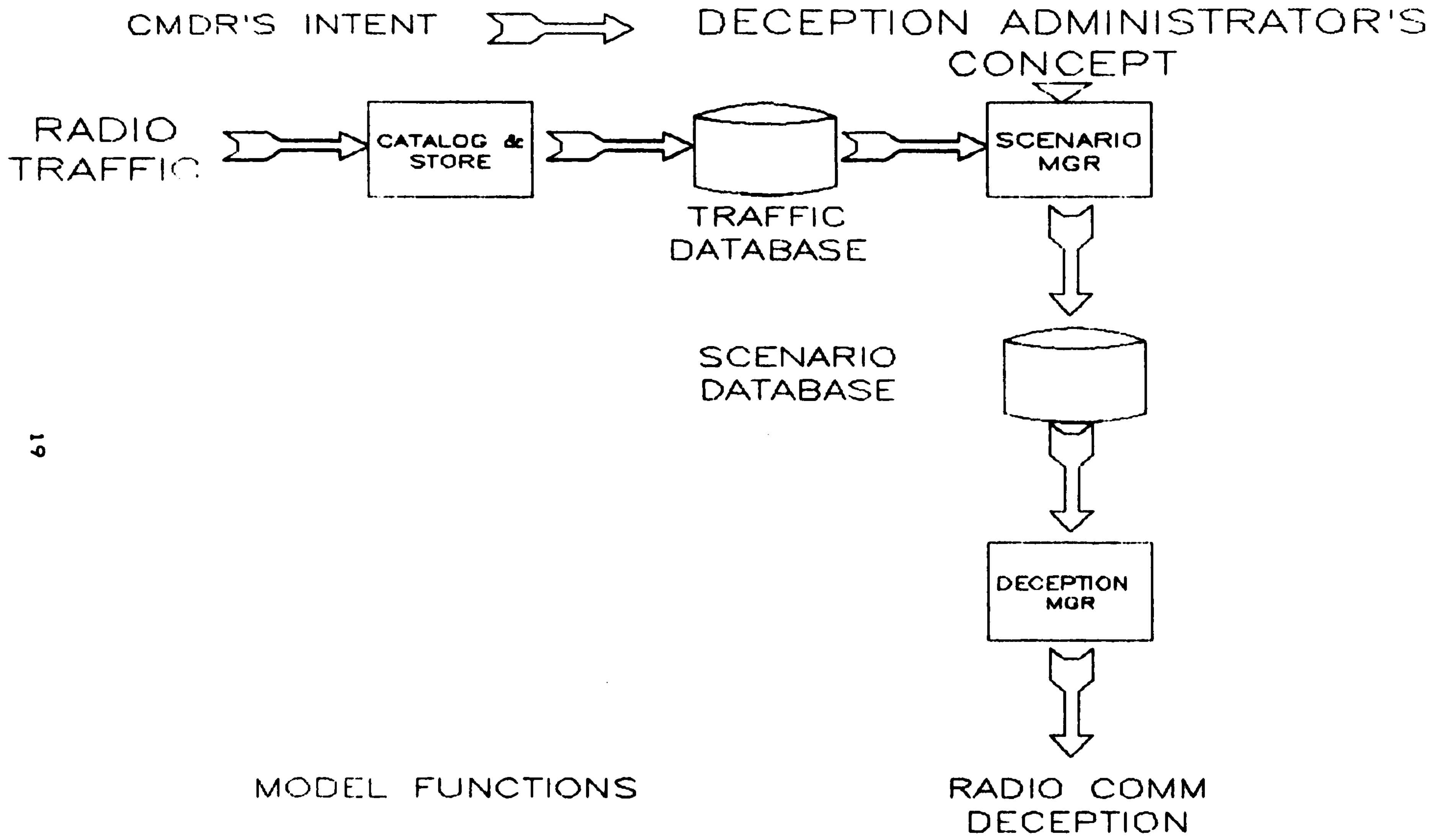
Together, these three faculties constitute the functionality of the proposed model. However conceptual in presentation, no automated system designed to perform an automated radio communications deception would be able to operate without the basic tasks of storing data, building scenarios and transmitting message traffic; these are fundamental to the model. Figure 3 shows how the three functions relate to each other. A presentation of the components of the model will demonstrate how these functions relate to the overall workings of the model.

COMPONENTS OF THE MODEL

Refer to Figure 4 during the presentation of the various components of the proposed model.

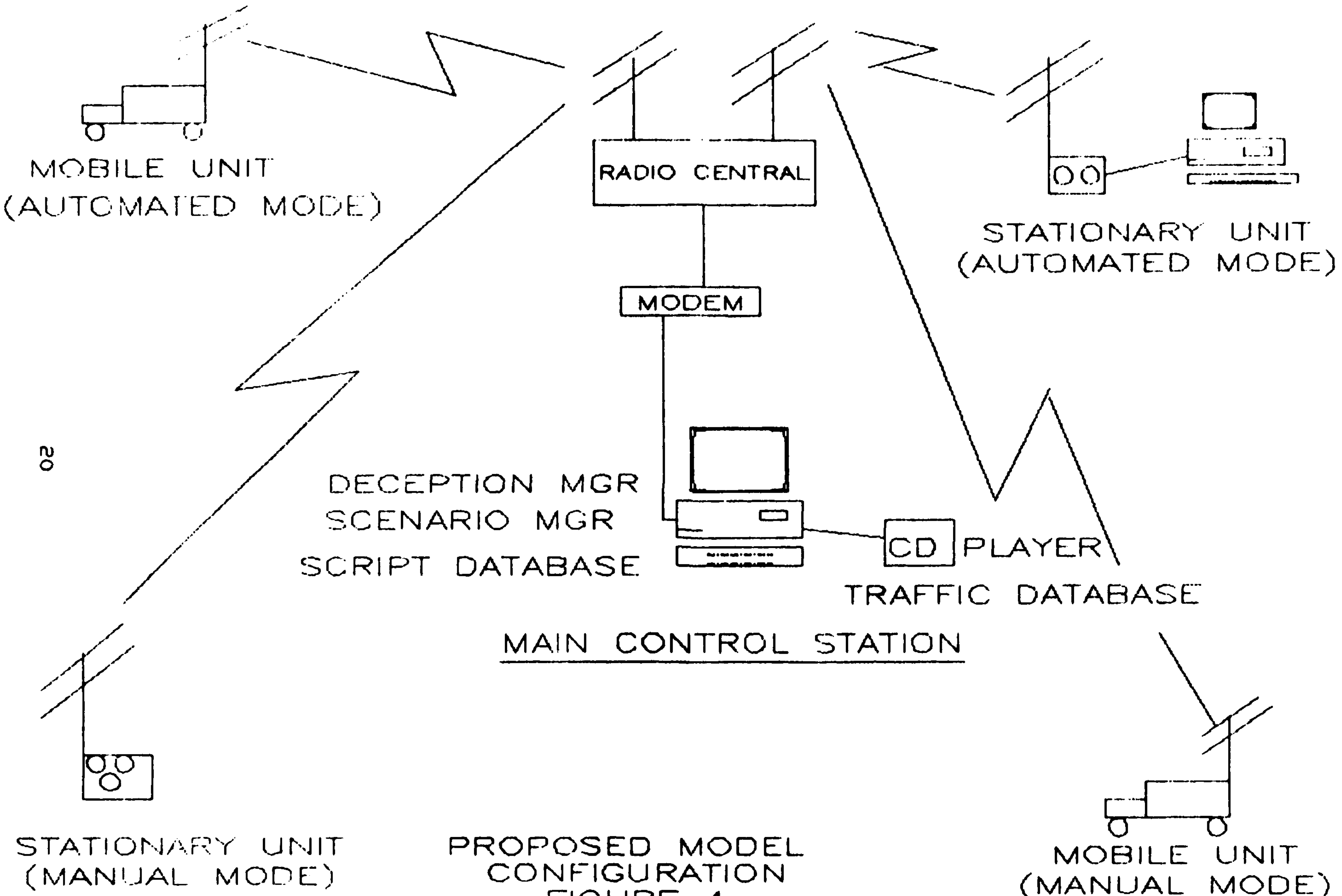
MAIN CONTROL STATION

During scenario formulation, this station uses the catalogue and store software and the scenario manager in building the traffic database and the scenario databases. Connected to a CD player which stores the traffic database, this station controls the deception during scenario execution by the propagation of control data and message traffic to all



MODEL FUNCTIONS

FIGURE 3



PROPOSED MODEL
CONFIGURATION
FIGURE 4

of the subnodes in the network. Radio assets, allotted for the deception, are concentrated in Radio Central. Both the Main Control Station and Radio Central could be mobile units (or ships for that matter) if the scenario is imitating a maneuver unit. MODEMS for digital to analog conversion and encryption devices are present in the model as necessary. For maximum flexibility, all components would operate on battery power alone. Once the scenario is initiated, there is no reason that the Main Control Station and fully automated subnodes couldn't operate unattended with only periodic maintenance required.

INTELLIGENT SUBNODES

Any station provided with a microcomputer, CD storage and player, modems and radios together with the proper software applications would constitute an automated subnode on the network. These stations could be either stationary or mobile depending on the scenario. Taking their instructions from the control data propagated by the Main Control Station, these subnodes would execute a subset of the deception scenario representative of the subordinate or adjacent unit they were programmed to imitate. During the formulation of the scenario database, subset databases would be created for use by these intelligent subnodes which would reflect the subnode's tasks. As was the case with Main Control, these nodes could also operate unattended once the deception was initiated.

MANUAL MODE SUBNODES

Resources may not allow for each node on the network to be allotted a full suite of automated equipment. Therefore, provision is made for the implementation of a node with the barest suite of radio equipment; possibly a radio set alone. In order to implement this type of subnode, the deception administrator will have to provide written scripts, based on the formulated scenario, to operators who would man these manual mode subnodes. This could be easily done by building the scenario as if the target node were an intelligent node and then playing back the scenario while transcribing the interaction onto a written script. These typed scripts, which would display both message traffic to be received and responses to be transmitted together with control information, constitute the traffic database in written form, for a manual subnode. Obviously, manual subnodes are attended by at least a minimum of personnel.

Equipment for the components of the model described above is resident in today's force. General purpose microcomputers would suffice for the control station and subnodes illustrated. Organic radio equipment needs no modification to be included in the network model. Obviously, the software applications described would require substantial design and development before any model implementation could be a reality.

CHAPTER IV

ADVANTAGES AND DISADVANTAGES OF THE MODEL

Economy of force facilitation is the main advantage of the proposed model. Given that the model is implemented in its fullest form, with attendant radio traffic databases representative of the operational level of warfare (corps, divisions, brigades, logistics bases, battle groups, etc.), large formations could be imitated in the conduct of a realistic deception with a minimum of manpower and time. Since scenarios would be developed and "canned" on digital storage media, deceptions could be formulated, tested and reviewed for applicability prior to their use; usually by someone other than a member of the command requesting the deception application. Because in the future, manpower resources will be increasingly at a premium, having a tool which can conduct a large scale communications deception without undue requirements for scenario designers or operators would provide great flexibility to an operational commander and his staff.

The proposed model addresses each of the elements, described in Appendix I, which are fundamental to the conduct of a practical radio communications deception. Because of the microcomputer's inherent ability to follow a set sequence of instructions contained in a software program, elements such as tempo, volume, patterns and synchronization can be specified in program parameters based on experience with manual deceptions. The computer's ability to store and manipulate data and drive external peripheral electronic devices provide for great power in the control of a scenario. Properly designed databases and networks would result in realistic communications signatures and footprints.

Over time, the cataloging of numerous scenarios would provide a library of "off-the-shelf" communication deceptions which could be deployed with an operational command for use in a wide array of operational situations. It is this feature which recommends the proposed model over the current practices of the art.

There are two general types of overhead associated with the model which are not insignificant. The first is a one-time system developmental cost that is related to the design, construction and implementation of the software applications that make up the system. There are aspects of the model which will require significant analysis and technical expertise in their design. For instance, the application which assembles scenarios out of the stored and catalogued building block message traffic (the scenario manager) is not a simple program to design and develop. Understanding that similar systems development efforts have failed dismally due to unsatisfactory specification and "gold plating", concern is valid as it relates to this issue.

Secondly, there is cost associated with the gathering and storage of message traffic and the construction of deception scenarios should the model ever be implemented. It's quite conceivable that an agency would have to established just to build traffic databases and scenarios on order. It's difficult to imagine an operational unit being able to do this on their own given their resources on hand and considering that it appears that database construction and scenario fabrication are very manpower intensive. Certainly testing, evaluation and certification of a given scenario would be very costly in time and effort. It's possible that I'm overstating this disadvantage in that software could be designed to ease the burden of this activity but, this aspect of the model bears thought and consideration and should not be taken lightly.

CHAPTER V

CONCLUSION

Humans have been attempting to deceive their enemies in warfare since the dawn of time. Efforts as diverse as the Trojan Horse ploy and the FORTITUDE SOUTH operation conducted to deceive Hitler as to the location of the invasion of France exemplify mankind's expenditure of ingenuity and resources in the quest to mislead foes. Just as with the constant attempt to dominate the battlefield though the alternating power of offense and defense, there is one thing that is constant in the deception game and that is the continuing application of leading edge technology to deception methods. Certainly, simple, low-tech deceptions have their place in tactical situations - the slick, modest ploy taken hook, line and sinker by an enemy can produce great benefits in individual battles and engagements. But, at the operational level of war, the application of technology to deception comes to the fore. Radar, imagery, and electronic communications provide fertile ground to the commander seeking to deceive his enemy on a grand scale.

In comparison to most military disciplines, few automated war fighting tools are at an commander's disposal at the operational level of warfare. As relates to the functional area of operational deception, I could find no automated system available for deception execution and only one, in the design stage, for deception planning. Given the advanced state of microcomputer and communications technologies in this country and the significant benefits that timely and realistic radio communications deception might lend to an operation, it is lamentable that more has not been done. Since the effort to develop and implement a deception tool such as the one proposed in the model is not minor, it would take the interest of personnel at the service level to initiate progress towards that goal. It is the opinion of this researcher that the effort would be worth it.

As Professor Handel makes clear in his book on modern day deception, the only commanders that can practice the art of deception are those who are willing to delegate much authority to a small group of people whom they have great confidence in.[6] If that group of people is in possession of a powerful set of deception tools, the commander's confidence will be rewarded.

APPENDIX I

ELEMENTS OF ELECTRONIC RADIO COMMUNICATIONS DECEPTION

ELEMENTS OF EFFECTIVE RADIO ELECTRONIC DECEPTION

Little or nothing is written in the literature on the elements of electronic deception that could be used as an aid in the design of the model. Appendix B of FM 90-2 is titled "Ideas and Techniques for Electronic Deception" but, it provides only general guidance and most of that is directed at radars and jamming.[7]

This appendix will therefore attempt to outline the most important elements of radio electronic communications in order to construct a baseline for the proposed model. The elements described are submitted as key components of Manipulative Electronic Deception (MED). MED is defined formally in FM 90-2 as:

> "The use of friendly electromagnetic radiation to falsify information an enemy can obtain from analyzing electromagnetic radiation."[8]

For the purposes of the model, MED will be considered in the context of the employment of a microcomputer-based system for the collection, management, control and dissemination of radio communication traffic in order to provide the enemy with a false impression of the friendly situation. The elements of MED which are considered germane to the proposed model are presented as follows:

SCENARIOS

Scenarios are fundamental to the prosecution of a comprehensive, and therefore believable, electronic deception. Through the use of radio traffic, they present a series of events which, by their interception, are meant to mislead the listener. No hodge-podge of radio traffic, thrown together at the spur of the moment, will suffice for a meaningful deception effort. Moreover, the scenarios must be tailored to the size, composition, activity and, in some cases, to the location, of the unit which is being imitated. This is important for the campaign planner who may be required to think in corps, division, squadron, wing and battle group components of the force.

Scenarios are not static in time. An inclusive scenario will be orchestrated in time driven events. A scenario is simply the story line laid out in time and space.

SCRIPTING

Scripting is a subset element of scenarios. In today's manual attempts at radio communications deception, a written script (often hand written) is sometimes used to drive the conduct of the deception. At other times, free play, using real or exercise radio traffic, is used to radiate radio emissions. Regardless of how it is implemented, some design is necessary for the deception scenario. If the entire script can be designed, reviewed, optimized and stored for future use, all the better for the commander who would utilize it for deceptions.

SIGNATURES

Consider the signature element for a unit as the equivalent of the fingerprint on a human being - each one is distinct and almost impossible to counterfeit. Everything which would distinguish the organization via the airwaves, including the voices of the radio operators, the callsigns and frequencies used by the unit, the writing style of the staff and commanders and the pattern of communications is included in the signature of the unit.

FOOTPRINTS

This element addresses the unit's placement, positioning and relationship to other units on the ground or on the sea.

CONTENT

Radio traffic must contain the verbiage and the format coincidental with the unit that is being imitated. This is especially true if some, and maybe all, of the traffic is to be broadcast in the clear.

VOLUME

An emulation must be capable of putting out sufficient quantities of radio traffic commensurate with the size and the mission of the unit.

DIVERSITY

There are numerous types of units within any large organization and they each have different things to transmit which take different amounts of time on radio nets. If a commander orders the imitation of a certain type of unit, the radio traffic should contain the diversity of traffic which is normally associated with the unit to include its staff functions.

PATTERNS

Radio traffic flows in certain patterns usually described by the communications network employed to support an operation.

SYNCHRONIZATION

It is possible to discern radio traffic events which coincide, in time, within the patterns attributable to a particular unit. Traffic queues are based on the operational event at hand, the time of day and the message received which requires response.

TEMPO

Radio events happen at a certain speed depending on the unit radiating. Radio traffic analysis considers the pace of emissions when determining the type and activity of a unit under surveillance.

REALISM

All of the above noted elements, if combined properly, result in a realistic foundation for electronic deception using radio communications.

CONTROL

Central control requirements for the large scale deception operation rise almost exponentially with the unit size. No amount of scripted, pre-planned radio messages can be made to substitute for positive, real-time control from a agency that understands the requirements for the elements that make up a practical deception. Control is the one operational component of a radio communications deception that is difficult to train at and rehearse. This is so because the human and equipment resources are not available for such training because they are usually dedicated to normal mission type training operations.

ENDNOTES

1. Tzu, Sun. The Art of War. Trans: Samuel B. Griffith. Oxford: Oxford University Press, 1963, pg. 106.

2. Clausewitz, Carl von. On War. Trans: Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976, pg. 203.

3. Handel, Michael I. "Sun Tzu and Clausewitz: The Art of War and On War". Professional Readings in Military Strategy No. 2. U.S. Army War College, Carlisle Barracks, Penn, 1991, pg. 43.

4. Cave-Brown, Anthony. Bodyguard of Lies. New York: Harper and Row, 1975, pg. 461.

5. Clausewitz, pg. 203.

6. Handel, Michael I. Military Deception in War and Peace. Jerusalem: Magnus Press, The Hebrew University, 1985, pg. 28.

7. Department of the Army. Tactical Deception. FM 90-2. Washington, D.C., August, 1978. pp. B-1 to B-4. UNCLASSIFIED.

8. Ibid, pg. 2-16.

BIBLIOGRAPHY

Ackerman, Robert K. "The Art of Deception". SIGNAL, September, 1988, pp. 47-51.

Brown, Margaret L. "Operational Deception During World War II: How Big Was Its Role?". Unpublished Research Paper, Naval War College, Newport, RI, 1990.

Cave-Brown, Anthony. Bodyguard of Lies. New York: Harper and Row, 1975.

Clausewitz, Carl von. On War. trans: Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Department of the Army. Operations. FM 100-5. Washington, D.C., August, 1978. UNCLASSIFIED.

Department of the Army. Tactical Deception. FM 90-2. Washington, D.C., August, 1978. UNCLASSIFIED.

Dewar, Michael. The Art of Deception in Warfare. Newton Abbot, Devon, England: David and Charles, 1989.

Flowers, Russell B. "Cover and Deception: A Lost Art?". Unpublished Research Paper, Naval War College, Newport, RI, 1990.

Handel, Michael I. Military Deception in War and Peace. Jerusalem: Magnus Press, The Hebrew University, 1985.

Handel, Michael I. ed. Strategic and Operational Deception in the Second World War. London: Frank Cass and Co., Ltd., 1987.

Handel, Michael I. "Sun Tzu and Clausewitz: The Art of War and On War". Professional Readings in Military Strategy, No. 2. U.S. Army War College, Carlisle Barracks, Penn, 1991.

Lord, Walter, Incredible Victory, McGraw-Hill, New York, NY, 1981.

Tzu, Sun. The Art of War. trans: Samuel B. Griffith. Oxford: Oxford University Press, 1963.